UNITED STATES DISTRICT COURT
DISTRICT OF VERMONT

IN THE MATTER OF THE SEARCH OF 700 RIVERSIDE AVENUE, APARTMENT H, BURLINGTON, VERMONT	Case No. 2:22-MJ-117 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Joshua Otey, being first duly sworn, hereby depose and state as follows:

I. Introduction

A. Affiant

1. I am a Special Agent with Homeland Security Investigations, Department of Homeland Security ("HSI"), currently assigned to HSI's Burlington Office. I have been a Special Agent with HSI since March 2020. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of Title 18, United States Code, Sections 2251, 2252, and 2252A. I have participated in a number of investigations into the receipt, possession, and/or distribution of child pornography by electronic means. I have gained expertise in these areas through training and daily work related to conducting these types of investigations. I also have experience executing search warrants, including search warrants for physical premises and electronic evidence.

2. I have personally participated in the investigation of the offense discussed below. I am familiar with the facts and circumstances of this investigation from my participation in the investigation, my review of documents, my training and experience, and discussions I have had

with other law enforcement personnel concerning the creation, distribution, and proliferation of child pornography.

3. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises specified below, further described in Attachment A, for the items and information described in Attachment B. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of computers and electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Premises

4. The premises to be searched (the "Subject Premises") is 700 Riverside Avenue Apartment H, Burlington, Vermont. 700 Riverside Avenue, Burlington, Vermont is a two-story red building with red siding and multiple apartment units. The Subject Premises is an apartment within the building having an entry on the 1st floor of the building and labeled "700-H" on an address marker above the entry door. The Subject Premises is described in more detail in Attachment A to this application.

C. The Subject Offense

5. For the reasons detailed below, I submit that there is probable cause to believe that the Subject Premises contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(2) & 2252A(a)(2) (receipt of child pornography) as well as

2252(a)(4) & 2252A(a)(5) (possession of child pornography) (the "Subject Offense"). 18 U.S.C. Sections 2252 and 2252A prohibit a person from knowingly possessing or accessing sexually explicit images (child pornography) with the intent to view them as well as transporting, receiving, distributing or possessing in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, any visual depiction of minors engaging in sexually explicit conduct (child pornography).

D. Terminology

6. As used herein, the following terms have the following meaning:

a. Child Pornography: defined in Title 18, United States Code, Section 2256(8) in pertinent part as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct . . ."[1]

b. Computer: includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, server computers, and network hardware, as well as wireless routers and other hardware involved in network and Internet data transfer.

c. Computer hardware: all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices) and peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d. Computer software: digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

---

[1] *See also Ashcroft* v. *Free Speech Coalition*, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

e. Computer Data/ESI (Electronically Stored Information): consistent with Fed. R. Crim. P. 41 and the Advisory Committee Comments to the 2009 amendments, ESI includes writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained, including all types of computer-based information as may be developed over time. "Computer data" as used herein is synonymous with ESI.

f. Computer Passwords, Pass-Phrases, and Data Security Devices: as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. Directory or Folder: a simulated electronic file folder or container used to organize files and directories in a hierarchical or tree-like structure.

h. File: a collection of related data or information stored as a unit under a specified name on storage medium. Not all ESI is stored in files.

i. File Extension: many operating systems allow a filename extension that consists of one or more characters following the proper filename. For example, image files are frequently stored as .bmp, .gif, .jpg, or .tiff; audio files commonly come in a variety of formats such as .aud, .wav, or .mp3. The filename extension should indicate the file type or format; however, users may change filename extensions to evade firewall restrictions or for other reasons. Accordingly, file types must be identified at a binary level or by viewing the contents of the file, rather than by relying on file extensions alone.

j. Forensic Copy/Image Copy: a data compilation created with the use of forensic software that contains an exact copy, sometimes referred to as a bit-by-bit copy, of an entire physical storage medium (hard drive, smart phone, DVD, tape, etc.), including all active and residual data and unallocated or slack space on the media. Forensic copies are sometimes called "images" or "imaged copies" or "mirror images." Forensic copies are generally only reviewable via forensic review software (meaning that user files contained within a forensic copy cannot simply be opened with the program originally used to create them). User files can, as useful, be extracted from forensic copies for ease of review; but review of latent or residual data, where needed, must generally take place via forensic review software.

k. Internet: a global network of computers and other devices that communicate with each other. It supports services such as email, the World Wide Web, file transfer, and Internet Relay Chat. Due to the structure of the Internet, connections between devices on the Internet often

cross state and international borders, even when devices communicating with each other are in the same state.

l. Internet Protocol address ("IP Address"): a unique numeric address used to identify a particular computer connected to the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static — that is, long-term — IP addresses, while other computers have dynamic — that is, frequently changed — IP addresses.

m. Latent/Residual Data: deleted files and other ESI that are inaccessible without specialized forensic tools and techniques. Until overwritten, this data resides on media such as a hard drives in unused space and other areas available for data storage. It can include data within files that has functionally been "deleted" in that it is not visible using the application with which the file was created absent use of undelete or special data recovery techniques.

n. Metadata: data that describes characteristics of other ESI, for example, how, when, and by whom that ESI was collected, created, accessed, modified, and formatted. Metadata can be found in different places in different forms; it can be created by applications, users, or the file system; and can be altered intentionally or inadvertently. Some metadata, such as file dates and sizes, may be easily accessible; other metadata can be hidden or embedded and unavailable without technical skill and tools.

o. Records, documents, and materials: include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

p. Slack Space: space within a cluster (unit of storage space for a file) that is not being used for storage of the file, but which may contain latent or residual data relating to the file or to other activity on the computer.

q. Storage Medium, ESI Storage Device, ESI Storage Media, Electronic Storage Media: any device or physical object capable of storing ESI, including computers, optical disks such as CDs and DVDs, RAM (random access memory), floppy disks, flash memory, thumb or flash or USB drives, tapes and cartridges, and other magnetic or optical media.

r. User File: a file generated by a user, generally by using a program or application such as a word processor or photo editor, as distinct from files constituting, or generated by, the system or program.

s. "Minor," "Sexually Explicit Conduct" and "Visual Depiction": are defined as set forth in Title 18, United States Code, Section 2256.

II. Probable Cause

A. Probable Cause Regarding Commission of the Subject Offense

Technical Background

7. Through investigative research and through conversations with other individuals regarding Discord Inc. ("Discord"), your Affiant has learned that Discord is a messaging platform where millions of users from around the world connect with each other though chat, voice, and video. Discord stores messages and attachments that users send to each other in text channels, whether in a server or in direct messages. In general, Discord servers retain data to include messenger communication until the subscriber deletes the communication string. If the subscriber does not delete the message, the message can remain on Discord servers indefinitely. Even if the subscriber deletes the data, it may continue to be available on Discord servers for a certain period of time.

The Investigation

8. In or about August 2022, HSI Burlington received information from the Vermont Internet Crimes Against Children ("ICAC") taskforce and the New Jersey State Police ("NJSP"). A minor female twelve-year-old child ("MV1") had received sexually explicit communications as well as solicitation of nude images and videos, and had been subjected to threatening behavior by a subject over the social media platform Discord. It should be noted that MV1 is diagnosed with Autism. MV1 is located in Commercial Township, New Jersey.

9. On or about June 3, 2022, New Jersey State Police Detective Trooper Brian McGinn was assigned a child exploitation investigation. During the investigation Detective McGinn met with MV1 and her father. Investigation revealed MV1 was subjected to and complied with solicitation of nude image(s) and video(s) over Discord by a subject utilizing the username "nut#7363" and visible vanity name "nut" from approximately May 9, 2022, through approximately June 3, 2022.

10. Detective McGinn advised that during a review of the Discord conversation, "nut" introduced himself as a (13) thirteen-year-old and immediately began requesting MV1 to photograph herself in exchange for items on the "Roblox" game platform, to which she complied. MV1 had sent the subject "nut" nude photographs and videos of herself at their request. Although I have not reviewed these images, they have been reviewed by Detective McGinn and partially described below.

11. Detective McGinn advised that as the conversation progressed, the directions from "nut" to MV1 became increasingly sexual in nature, and ultimately, "nut" began to direct MV1 to perform sexual acts on herself and record them. For instance, on or about May 9, 2022, "nut" requested of MV1, "can you take a pussy pic sitting down on the toilet or something so i can see it spread open?" MV1 complied and sent "nut" an image that depicted herself in a seated position with her legs apart, exposing her vagina and inner thighs. Detective McGinn confirmed that the image depicted MV1, as an item of clothing in the image matched what MV1 had worn in a previous image. Subsequently, MV1 indicated to "nut" that she no longer wished to participate in the conversation and as a result, "nut" began to threaten her, specifically by stating that they would post the previously obtained images to her "Tik-Tok" platform. Following the threats, MV1 ultimately complied with the requests of "nut" and performed directed sexual actions while video

recording herself and sent the videos to "nut." Detective McGinn viewed videos of MV1 that had been sent to "nut," and described the video as depicting MV1 completely nude, manipulating her vagina in a sexual manner. Detective McGinn advised the conversation from "nut" following their receipt of said video was threatening and included a request for more sexual material. Detective McGinn advised that, at this point in the communications, MV1 blocked the subject "nut" after receiving threats that MV1's images and videos would be shared. After being blocked, "nut" began messaging friends of MV1 and threatened her through her friends, including providing a screen shot of MV1's location obtained through the identification of her IP address with what Detective McGinn described as a significant degree of accuracy.

12. MV1 told Detective McGinn that she knew the subject "nut" to use the vanity name "@Deyquan" on the "Roblox" platform.

13. On June 9, 2022, an audio/video recorded forensic interview was conducted of MV1 by Detective Kahn of the Cumberland County Prosecutor's Office. I have reviewed this interview which was also documented in a report by Detective McGinn and Detective Kahn. During the interview, MV1 stated the following in sum and substance. While playing "Roblox" she was approached by a subject, who she identified as "nut," and who convinced her to communicate with them on "Discord." MV1 said that during the conversation, "nut" directed her to send pictures and videos of herself.

14. Detective McGinn served legal process and exigency requests upon service providers including Discord, Comcast, and T-Mobile. A review of information provided by the service providers and conversations with Detective McGinn revealed the following in sum and substance.

a. I have reviewed records from the social media platform Discord for the username "nut#7363." These records show that, from at least September 17, 2017, until at least on or about June 21, 2022, the Discord username "nut#7363" was associated with their service. The subscriber records for the account revealed an associated email address odercraftyt@gmail.com and an associated telephone number (802) 304-9678. Additionally, Discord provided IP address information associated with the user account, including 24.91.160.42 (a query of American Registry of Internet Numbers (ARIN) revealed this IP address is associated with the internet service provider Comcast), and 172.58.217.129 (a query of American Registry of Internet Numbers (ARIN) revealed this IP address is associated with the internet service provider T-Mobile).

b. Legal process served upon Comcast caused the production of records. I have reviewed records from the Internet service provider Comcast for the IP address 24.91.160.42 identified in paragraph 14(a). These records show that, from at least May 28, 2022 through June 23, 2022, the IP address 24.91.160.42 was assigned to the subscriber account of "Deyquan Marty," with a service and billing address of 700 Riverside Avenue Apartment H, Burlington, Vermont, the Subject Premises. A telephone number associated with the Comcast account is (802) 355-4538 (a query of the telephone number through a free phone look up tool ZETX revealed the phone number is affiliated with the carrier ATT mobility),

c. I have reviewed records from cellular telephone service provider T-Mobile for the telephone number (802) 304-9678 identified in paragraph 14(a). These records show that the telephone number (802) 304-9678 is registered to the subscriber account of Deyquan Martin, with the address 126 North Avenue, Burlington, Vermont. An additional contact number is listed

on the account for Martin as (802) 355-4538 which is identified as the contact telephone number for the Comcast account referenced in paragraph 14(b).

15. On September 9, 2022, an administrative subpoena was served upon AT&T for records associated with the telephone number (802) 355-4538. I have reviewed records from cellular telephone service provider AT&T, which revealed the following in sum and substance: The number was registered to the subscriber account of Deyquan Martin, with the address 126 North Avenue, Burlington, Vermont at the time of above-noted activity under investigation. Records revealed the account was active from December 14, 2018, through June 15, 2022, when the account was listed as "Final Disconnect."

16. On September 12, 2022, an administrative subpoena was served upon ROBLOX Corporation for records associated with the username @Deyquan as identified in paragraph 12. I have reviewed records provided by ROBLOX Corporation, which revealed the following in sum and substance: The username was assigned to the account of Deyquan MARTIN with a listed address of 126 North Avenue, Burlington VT. The account was created on February 7, 2011. Email accounts associated with the account are TheWeirdpeep@gmail.com and dqm2009@aol.com. Billing account information includes a "charge card" on file listed as 432855XXXX6505 with a billing email address of cheetohead1337@gmail.com.

17. A query of Vermont Law Enforcement records for Deyquan Martin revealed numerous involvement records including but not limited to a prior investigation by the Vermont Attorney General's Office and the Vermont Internet Crimes Against Children (ICAC) taskforce related to child exploitation allegations. A review of law enforcement records revealed the address for Martin as 700 Riverside Avenue, Apartment H, Burlington, Vermont, the subject premises.

18. On August 22, 2022, a query of the Vermont Department of Motor Vehicles revealed Deyquan Martin lists an address 126 North Avenue, Burlington, Vermont. The record revealed Martin has no Vermont Driver's License on-file.

19. On September 14, 2022, I contacted Steven Offenhartz who is the owner of Offenhartz Management which is the managing member of BRI Properties LLC. BRI Properties LLC owns 700 Riverside Avenue, Burlington, Vermont. Steven Offenhartz confirmed that Deyquan Martin is a tenant of 700 Riverside Avenue, Apartment H, Burlington, Vermont and subsequently provided a Lease Agreement and Renewal Agreements listing Deyquan Martin and Gabrial Todd as tenants of 700 Riverside Avenue, Apartment H, Burlington, Vermont. The Lease Agreement indicates that Deyquan Martin and Gabrial Todd leased the Subject Premises effective November 27, 2020 for six months. The Renewal Agreements indicate that Deyquan Martin and Gabrial Todd renewed the Lease Agreement for one year effective July 26, 2021 and for another year effective July 26, 2022.

B. Probable Cause Justifying Search of the Subject Premises

20. I have reviewed records from the Internet service provider Comcast for the IP Address 24.91.160.42 as identified in paragraphs 14(a) & 14(b). As noted above, these records show that, from at least May 28, 2022 through June 23, 2022, the IP address 24.91.160.42 was assigned to the subscriber account of "Deyquan Marty," with a service and billing address of 700 Riverside Avenue Apartment H, Burlington, Vermont, the Subject Premises.

21. I have also reviewed Vermont Law Enforcement records showing the address for Deyquan Martin as 700 Riverside Avenue, Apartment H, Burlington, Vermont, the Subject Premises. The last identified law enforcement contact with Deyquan Martin was July 1, 2022, when Burlington Police Detective Corporal Chenette served a subpoena upon him with a listed address of the Subject Premises.

22. Based on my training, experience, and conversations that I have had with other federal agents and law enforcement officers, I have learned the following:

a. Child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography usually do so by ordering it from abroad or through discreet contacts, including through the use of the Internet, with other individuals who have it available or by accessing web sites containing child pornography. Child pornography collectors often send and receive electronic communications conversing with other collectors in order to solicit and receive child pornography.

b. I know that people who collect and trade child pornography typically do not destroy or delete image files or video files depicting child pornography. Instead, collectors of child pornography typically retain their materials and related information for many years, and sometimes indefinitely. Even when files are deleted from a computer, they can frequently be recovered during a forensic examination.

c. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. Such individuals in possession of files containing child pornography are likely to save and maintain these files on their computers or other portable storage devices so they are readily accessible in their home, office, or vehicle.

d. Because of the illegality and the severe social stigma child pornography images carry, these individuals hide them in secure places. These secure physical places often include physical places such as the home or other structures on the property where the individual resides. These secure physical places can also include secure electronic places such as hidden files

on the hard drives of the individual's computers, external storage media, including but not limited to cellular phones or thumb drives.

e. I also know that collectors of child pornography often maintain lists of names, addresses, telephone numbers, and screen names of individuals with whom they have been in contact and who share the same interests in child pornography.

f. I am also aware that an individual who possesses more than one computer or smart phone may send a file containing child pornography from one phone to another phone or from one laptop to another in order to maintain, preserve and/or hide the file.

23. In light of the foregoing, information in support of probable cause in child pornography cases is less likely to be stale because collectors and traders of child pornography are known to store and retain their collections and correspondence with other collectors and distributors for extended periods of time.

24. Based on my training and experience, I know that persons who collect and distribute child pornography frequently collect and view sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification. These examples of visual media containing sexually explicit materials are often times stored on various devices, including but not limited to, computers, disk drives, modems, thumb drives, personal digital assistants, mobile phones and smart phones, digital cameras, and scanners, and the data within the aforesaid objects relating to said materials.

25. Based on the foregoing, I respectfully submit that there is probable cause to believe that someone located at the Subject Premises is engaged in the commission of the Subject Offense, and that evidence related to the Subject Offense may be found at the Subject Premises and within

and upon computers, cellphones, electronic storage media, and other electronic devices capable of storing data, information, and images.

C. Probable Cause Justifying Search of ESI

26. Individuals who engage in the criminal activity described herein, in the event that they change computers, will often back up or transfer files from their old computers' hard drives to that of their new computers, so as not to lose data, which would be valuable in facilitating their criminal activity. In addition, individuals who engage in such criminal activity will often also store or transfer files on electronic storage media other than computer hard drives, including thumb drives, flash memory cards, CD-ROMs, or portable hard drives to, for example, facilitate the use of the information or to transfer it to co-conspirators in support of the criminal scheme.

27. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files can be stored on a hard drive for years at little or no cost. Even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. Specifically, when a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Deleted files, or remnants of deleted files, may accordingly reside in "slack space" (see supra ¶ 6(q)) for long periods of time before they are overwritten. In addition, a computer's operating system may keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are generally automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was

downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

28. Based on the foregoing, I respectfully submit there is probable cause to believe that someone located in the Subject Premises is engaged in the Subject Offense, and that evidence of this criminal activity is likely to be found in ESI recovered at the Subject Premises.

III. Procedures for Searching ESI

A. Execution of Warrant for ESI

29. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review." Consistent with Rule 41, this application requests authorization to seize any computer devices and storage media and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.
- Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.
- Third, there are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.
- Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

B. Accessing ESI

30. The seized devices may include smartphones that offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") or facial recognition in lieu of a numeric or alphanumeric passcode or password. For Apple devices, for example, this feature is called Touch ID or Face ID, depending on the model of the Apple device.

31. If a user enables Touch ID on a given Apple device, he or she can register up to five fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) found at the bottom center of the front of the device. Similarly, Face ID allows a user to unlock the iPhone X and later models. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of the user's face. Face ID confirms attention by detecting the direction of the user's gaze, then uses neural networks for matching and anti-spoofing so the user can unlock the phone with a glance. Face ID automatically adapts to changes in the user's appearance, and carefully safeguards the privacy and security of the user's biometric data.

32. In my training and experience, users of mobile devices that offer security technology like Touch ID and Face ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

33. In some circumstances, a fingerprint cannot be used to unlock a device that has security technology like Touch ID enabled, and a passcode or password must be used instead. These circumstances may include: (1) the device has been turned off or restarted; (2) the device has received a remote lock command; (3) five unsuccessful attempts to unlock the device via Touch ID are made; (4) when more than 48 hours has passed since the last time the device was unlocked; and (5) when the device has not been unlocked via Touch ID in eight hours and the passcode or password has not been entered in the last six days.

34. Similarly, in some circumstances, the user's face cannot be used to unlock a device that has security technology like Face ID enabled, and a passcode or password must be used instead. These circumstances may include: (1) the device has just been turned on or restarted; (2) the device has not been unlocked for more than 48 hours; (3) the passcode has not been used to unlock the device in the last 156 hours (six and a half days) and Face ID has not unlocked the device in the last four hours; (4) the device has received a remote lock command; (5) after five unsuccessful attempts to match a face; (6) after initiating power off/Emergency SOS by pressing and holding either volume button and the side button simultaneously for two seconds. Thus, in the event law enforcement encounters a locked mobile device, the opportunity to unlock the device via fingerprint or face recognition exists only for a short time.

35. The passcodes or passwords that would unlock any smartphones seized in connection with this warrant are not known to law enforcement. Thus, it may be necessary to press the fingers of someone found in the Subject Premises, to any smartphones seized in connection with this warrant in an attempt to unlock the device(s) for the purpose of executing the search authorized by the warrant sought by this Affidavit. Similarly, it may be necessary to have someone found in the Subject Premises remain still and look, with eyes open, at the camera of any

smartphones seized in connection with this warrant in an attempt to unlock the device(s) for the purpose of executing the search authorized by this warrant. Attempting to unlock any smartphones seized in connection with this warrant with the use of the user's fingerprints or face may be necessary because the Government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by the warrant being sought.

36. Although I do not know whether any smartphones will be seized in connection with this warrant or whether any fingerprints of anyone found in the Subject Premises will be capable of unlocking any of such devices, based on my training and experience I know that it is common for users to unlock their devices via the fingerprints on their thumbs or index fingers. In the event that law enforcement is unable to unlock any smartphones seized in connection with this warrant within the number of attempts permitted by the devices' security features, this will simply result in the devices requiring the entry of a password or passcode before it can be unlocked.

37. I therefore request that the Court authorize law enforcement to press the fingers, including thumbs, of individuals found in the Subject Premises to any smartphones seized in connection with this warrant, or to instruct the individuals found in the Subject Premises to remain still, with eyes looking forward at the camera of any smartphones seized in connection with this warrant, for the purpose of attempting to unlock the devices in order to search the contents as authorized by the warrant sought by this Affidavit.

IV. Conclusion and Ancillary Provisions

38. Based on the foregoing, I respectfully request the court to issue a warrant to search the Subject Premises, described in Attachment A, and to seize and search the items described in Attachment A.

39. In light of the confidential nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the

Court orders otherwise. The Government is not requesting delayed notice, however, and will leave a copy of the search warrant and the return at the Subject Premises.

JOSHUA OTEY
Special Agent
Homeland Security Investigations

Sworn to and subscribed before me this 16th day of September ___, 2022

HONORABLE JUDGE KEVIN DOYLE
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF VERMONT